HIPAA Implementation Newsletter
Issue #20 – October 19, 2001
Web format with links at http://lpf.com/hipaa
Security: Internet | Microsoft | Web Sites | Web Audit | Public Health | Costs |-| Paper Records

News coverage of the destruction of the World Trade Centers and portions of the Pentagon on September 11, is yielding to the anthrax scare and the war in Afghanistan. Security is now a major topic for us all. Timely for the moment and relevant for the foreseeable future.

_____Security: Internet_____

"The SANS Institute and the National Infrastructure Protection Center (NIPC) have released their second list of Most Critical Internet Security Vulnerabilities. … This new list, released on October 1, 2001, updates and expands the Top Ten list. With this new release, we have increased the list to the Top Twenty vulnerabilities, and we have segmented it into three categories: General Vulnerabilities, Windows Vulnerabilities, and Unix Vulnerabilities.

"The SANS/FBI Top Twenty list is valuable because the majority of successful attacks on computer systems via the Internet can be traced to exploitation of security flaws on this list. …These few software vulnerabilities account for the majority of successful attacks, simply because attackers are opportunistic – taking the easiest and most convenient route. They exploit the best-known flaws with the most effective and widely available attack tools. They count on organizations not fixing the problems, and they often attack indiscriminately, scanning the Internet for any vulnerable systems.

"In the past, system administrators reported that they had not corrected many of these flaws because they simply did not know which vulnerabilities were most dangerous, and they were too busy to correct them all. Some vulnerability scanners search for 300 or 500 or even 800 vulnerabilities, thus blunting the focus your system administrators need to ensure that all systems are protected against the most common attacks. The Top Twenty list is designed to help alleviate that problem by combining the knowledge of dozens of leading security experts from the most security-conscious federal agencies, the leading security software vendors and consulting firms, the top university-based security programs, and CERT/CC and the SANS Institute. A list of participants [is included in the document].

"Manual methods for checking a system to see whether it has each of the listed vulnerabilities are presented in this document. A more practical approach to finding the UNIX and Windows vulnerabilities – especially if you practice safe computing by checking every new system before you attach it to the Internet, and rechecking all your systems frequently – is to use an automated scanner. Bob Todd, the author of the free Internet scanner SARA,

has created a special version of SARA designed specifically to find and report on the status of vulnerabilities on the SANS/FBI Top Twenty list. SARA's Top Twenty Vulnerability scanner is being made available by the Center for Internet Security (www.cisecurity.org - members only). To request a copy, email info@cisecurity.org with the subject "Top Twenty Scanner." Several commercial vulnerability scanners may also be used to scan for these vulnerabilities, and the SANS Institute will maintain a list of all scanners that provide a focused Top Twenty scanning function, at www.sans.org."

http://66.129.1.101/top20.htm Note: a "Log of Updates" is also posted on this site.

_____Security: Microsoft_____

One of the three categories in the above article is "Windows Vulnerabilities." Microsoft has launched a new program with the slogan: ""We will not rest until your business is secure. Period." Their announcement reads, in part:

"Microsoft announces the Strategic Technology Protection Program (STPP). This two-phase program represents an unprecedented mobilization of Microsoft's people and resources to integrate product, services and support.

"Phase 1: Get Secure We will help you get secure right now. Here's how. … The Microsoft Security Tool Kit CD includes best practice guides, information on securing your system, and service packs and patches that can help ensure your system is protected against attacks. It also provides tools that Microsoft has developed to help you secure your systems and keep them secure." You can order the tool kit free or get it online from the Web site.

"Phase 2: Stay Secure
We are working proactively with our customers to define, install, and maintain secure, reliable computing environments over the Internet by: … Launching security readiness events for our customers around the world. Making it more manageable to "stay secure" by developing enterprise security tools, creating auto-update functionality via Windows Update, and by producing bi-monthly product roll-up patches. …

"Microsoft is committed to doing everything possible to make certain that every customer can work, communicate, and do business securely over the Internet."

http://microsoft.com/security/

_____Security: Web Sites_____

Information Security magazine, … conducted the survey from late July to early August and received responses from 2545 information security workers.

Nearly 50 percent of the companies surveyed experienced attacks against their Web servers from external sources in 2001, up from 24 percent in 2000, the study found. Nearly 90 percent were hit with worms, viruses, or Trojans.

Security threats from those inside the company were more varied and frequent, but somewhat less serious, the study found. Seventy-eight percent of respondents said that company employees had installed or used unauthorized software and 60 percent used company computers for unauthorized or illegal purposes.

http://www.pcworld.com/news/article/0,aid,65526,00.asp October 10, 2001

_____Security: Web Audit_____

"... A crucial way of addressing the need to protect the company Web site is to conduct a security vulnerability assessment (SVA)--a security audit or ethical penetration test, as an SVA is also known.

"Your infrastructure requires seamless information access so that you can deliver the level of service that your customers have grown to expect. Dealing with security vulnerabilities on your Web site and your internal networks is not an option.

"If an outside consultancy is performing a network SVA, they'll ask your CIO to sign a form which entitles them to do one. You can have this document reviewed by your legal counsel, and be sure there is a section that proclaims the audit results to be as confidential as possible. You don't want your audit report showing up as market data on a Web site without your prior consent.

"Prepare yourself by bringing all your security processes, procedures, and network maps to the audit interview. ... It is appropriate for at least one senior member of the management team, and one person knowledgeable about security and network technology to attend such a session. After the in-person audit interview is complete, they will want to schedule up to a week's time to perform the penetration test on all your networks, and possibly longer depending upon the size of your network infrastructure. ...

"... A best-of-breed SVA usually starts out by doing some data gathering, and looking for reconnaissance information. ... Other kinds of things they will try will be checking include an assortment of vulnerabilities associated with file transfer protocols, hardware peripherals, hacker Trojans and backdoors, SMTP and messaging problems, network file system vulnerabilities, Web site and CGI holes. ...

"Make sure you receive a copy of the report, and make sure it ... summarizes, in ranked order, the potential threats, as well as the recommended action to take to reconcile the vulnerability. Your team can then work on reconciling

as many of the vulnerabilities as possible and then determine what they are unable to resolve. In the end, you can decide if it makes sense to hire an outside consultancy to resolve the final outstanding issues.
A SVA demonstrates your management's due diligence. … It does not, however, guarantee that your site cannot be successfully attacked or compromised. …"

http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2817146,00.html

_____Security: Public Health____

A recent report by HealthKey states: "Collaboration among the government, IT vendors, healthcare providers, and health plans reduced the average time it took to report an infectious outbreak to the Centers for Disease Control and Prevention (CDC) from over six weeks to a matter of days – replacing the old system of faxing information with a standardized and secure e-mail solution." This is a particularly timely in light of the recent anthrax cases. It should be noted that news about anthrax is clearly moving quickly.

The report describes a number of tests of technology for the transmission of secure data. We have added a link to the report: "The National HealthKey Collaborative: Securing the Exchange and Use of Electronic Health Information to Improve the Nation's Health—A Summary Report to the Community, September 2001" and the participating organizations; see "Update" near the end of this issue. The HealthKey project is funded by The Robert Wood Johnson Foundation.

http://www.healthkey.org/index.htm

_____Security: Costs_____

The final security rule is expected to give providers 24 months to comply. But the 498-bed St. Elizabeth's Hospital in Belleville, IL didn't think it would have the resources to implement new security technologies that quickly. So, it decided to jump the gun, says Donald Woeltje, senior network engineer.

"There's no way we can do it in 24 months starting from scratch," he says. "So we got started 18 months ago." Thus far, St. Elizabeth's has purchased and implemented anti-virus software and four suites of firewall software to protect e-mail servers, Web sites and the hospital's internal network from outside intrusion.

"To date, the hospital has spent about $100,000 for security technology, he estimates, and could spend up to $350,000 more to complete the work. Most of the additional money will go toward expanding use of security technology it already has enterprise wide."

http://www.healthdatamanagement.com/html/current/CurrentIssueStory.cfm?PostI

D=9056 October 2001 Issue

_____Paper Records: Designing_____

Yes Virginia, there are topics in addition to security.

Electronic medical records are electronic versions of paper records. They consist of scanned images of paper documents and occasionally include some information input directly into the computer. Donna Bowers, JD, RHIA, vice president at Baylor University Medical Center, in Dallas, TX suggested establishing these criteria for forms:

* White background only
* Standard paper size
* Use of only the front side of a page
* A standard area on every form for patient, hospital, and form identification

While developing additional criteria, it's a good time to decide whether each form is even necessary. Also, check to see what, if anything, your state laws say about what constitutes the legal medical record, and make sure your policy is developed in accordance with that. You'll also need to develop policies for:

* How long you'll retain records, both the paper and electronic versions
* Who can access the electronic medical records and paper records
* How records will be destroyed

Do not to keep the paper versions of records longer than necessary.

Some forms require a significant amount of information that is already in a computer. We suggest you consider using the computer to print these forms with the data already printed. The cost for the form will be higher than a pre-printed form but the data will be more accurate, revisions can be clearly indicated so you won't have to resolve discrepancies between data entered on the form and data already in the computer, people's time will be saved (may offset the added printing cost), and most people will appreciate the added service.

http://www.himinfo.com/ahima/2001/content_action.cfm?content_id=15661

_____Update_____

The Top 20 Internet Vulnerabilities have been added to the Privacy and Security page at:
http://lpf.com/hipaa/privacy-security.html#security-background-pands
The HealthKey report and participating organizations have been added

http://lpf.com/hipaa/privacy-security.html#transactions-messages-pands

_____

To be removed from this mail list, click:
mailto:hipaa@lpf.com?subject=remove
To subscribe, click: mailto:hipaa@lpf.com?subject=subscribe We appreciate it if you include information about your firm and your interests.

 Issues are posted on the Web at http://lpf.com/hipaa concurrent with email distribution. Past issues are also available there. Edited by Hal Amens hal@lpf.com

Information in the HIPAA Implementation newsletter is based on our experience as management consultants and sources we consider reliable. There are no further warranties about accuracy or applicability. It contains neither legal nor financial advice. For that, consult appropriate professionals.

Lyon, Popanz & Forester http://lpf.com is a management-consulting firm that designs and manages projects that solve management problems. Planning, program management offices and project management for HIPAA are areas of special interest.